

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) ) Case  
Property located at 405 Bishops Way, Apartment 223, ) No.23-880M(NJ)  
Brookfield, Wisconsin 53005 more fully )  
described in Attachment A. )

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Wisconsin  
(identify the person or describe the property to be searched and give its location):

Property located at 405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005 more fully described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before 4/24/2023 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

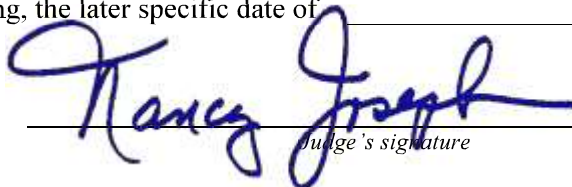
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: 4/10/2023 @ 2:33p.m

  
Judge's signature

City and state: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

## ATTACHMENT A

### **405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005**

405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005 is a residential unit in an apartment complex having a multi-colored stone structure, off-white colored trim, and a black and white roof. The numbers “405” are affixed to the apartment complex sign on the east side of the building. Apartment 223 is located on the second floor inside the apartment complex. The number “223” is displayed in black lettering next to the interior entrance door to the residential unit. Images of the exterior of the apartment complex and the entrance to Apartment 223 are below:



## **ATTACHMENT B**

### **Particular Things to be Seized**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, or property designed or intended for use or which is or has been used to assist in obtaining the means of committing criminal offenses, namely violations of Title 21 U.S.C. §§ 331(a) (interstate commerce of any misbranded drug), 331(c) (deliver of a misbranded drug), 331(d) (interstate commerce any unapproved new drug lacking FDA approval), Title 19 U.S.C. §§ 1595a(c)(1)(B) (unlawful importation), and Title 21 U.S.C. §§ 952 (importation of a controlled substance), hereinafter identified as the SUBJECT OFFENSES.

- a. Records and information relating to the purchase, sale, shipment, handling, importation, or distribution of Human Chorionic Gonadotrophin (“HCG”), and any other controlled substance, unapproved new drug products, misbranded drug products, and drug products unlawfully imported into the United States, including but not limited to prescriptions, bills, invoices, bills of lading, shipping documents, purchase orders, letters, notes, and order forms;
- b. Records and information, including literature, advertising, and labeling, related to the administration of HCG, any other controlled substance, unapproved new drug products, misbranded drug products, or drug products unlawfully imported into the United States, including related correspondence and communications;
- c. Records and information concerning the acquisition, retention, or distribution of HCG, any other controlled substance, unapproved new drug products, misbranded drug products, or drug products unlawfully imported into the United States, including related correspondence and communications;
- d. Records and information reflecting payment, receiving payment, or other transfer of funds in connection with the SUBJECT OFFENSES, including the acquisition, purchase, procurement, disbursement, or distribution of HCG, any other controlled substance, unapproved new drug products, misbranded drug products, or drug products unlawfully imported into the United States, such as checks, money orders, financial records, bank statements, currency, or other financial documents;

- e. Firearms, ammunition, cases, or firearm accessories and documents showing firearm possession or ownership, to include but not limited to CCW permit and firearm purchase/acquisition documents;
- f. Indicia of unlawful possession, use, or distribution of controlled substances and prescription medication, including but not limited to paraphernalia and evidence known to be associated with drug trafficking and/or drug possession;
- g. USPS packages or boxes;
- h. Evidence of recent cash expenditures;
- i. Information regarding identification and location of assets obtained with drug proceeds;
- j. Documents or other items pertaining to the controlled substance and prescription medication customers;
- k. All records, items, and documents reflecting travel for the purpose of participating in the aforementioned criminal offense, including but not limited to gas station receipts, store receipts, credit card receipts, restaurant receipts, maps, and records of long distance calls reflecting travel;
- l. All computers, tablets, and cellular telephones which may have been used by Kahled SALEM which may contain travel records, contacts with other individuals, email or social media contacts, or other records or communications related to the SUBJECT OFFENSES;
- m. Accounting records, specifically financial statements, bank records, ledgers, journals, check registers, and other books and records used to maintain a record of income and expenses;
- n. Checking, savings, and investment account records, including signature cards, account statements, deposit receipts, withdrawal receipts, cancelled checks, money orders, cashier's checks, records of incoming and outgoing wire transfers, electronic funds transfer records, checkbooks, credit card records and receipts, including supporting documentation and schedules, and any other records of documents pertaining to the receipt, expenditure, or concealment of money;
- o. Any and all of the above listed evidence stored in the form of magnetic or electronic coding on computer media or media capable of being read by a computer or with the aid of computer-related equipment, including but not limited to floppy disks, fixed hard

- disks, removable hard disks, tapes, laser disks, videocassettes, CD-ROM's, DVD disks, Zip disks, smart cards, memory sticks, memory calculators, personal digital assistants (PDS's), cell phones, and/or other media capable of storing magnetic coding, the software to operate them and related instruction manuals;
- p. All electronic devices which are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer impulses or data. These devices include computers, computer components, computer peripherals, word processing equipment, modems, monitors, printers, plotters, encryption circuit boards, optical scanners, external hard drives, and other computer related electronic devices;
  - q. All indicia of occupancy, residency or ownership of the premises and things described in the warrant, including identification documents, utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents, and keys.
  - r. Paraphernalia associated with the manufacture and distribution of controlled substances and prescription medications including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;
  - s. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;
  - t. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;
  - u. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;
  - v. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;

For any computer, cell phone, tablet, or storage medium (hereinafter, for purposes of this Attachment B, collectively referred to as a “COMPUTER”) whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the COMPUTER user’s state of mind as it relates to the SUBJECT OFFENSES;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;

- l. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment; and
- n. Routers, modems, and network equipment used to connect a COMPUTER to the internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "COMPUTER" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, flash memory, CD-ROMs, and other magnetic or optical media.



## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Property located at 405 Bishops Way, Apartment 223,  
Brookfield, Wisconsin 53005 more fully  
described in Attachment A.

Case No.23-880M(NJ)

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Property located at 405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005; more fully described in Attach. A.  
located in the Eastern District of Wisconsin, there is now concealed (identify the person or describe the property to be seized):

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 USC 331(a), 21 USC 331(d), 19 USC 1595a(c)(1)(B), 21 USC 952	interstate commerce of misbranded or new drugs lacking FDA approval, unlawful importation, and unlawful importation of a controlled substance

The application is based on these facts:

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

**Tyler Fink**

Digitally signed by Tyler Fink  
Date: 2023.04.10 12:10:38 -05'00'

Applicant's signature

Insp. Tyler Fink, USPIS

Printed name and title

Sworn to before me and signed in my presence.

Date: 4/10/2023

City and state: Milwaukee, Wisconsin

  
Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF A  
AN APPLICATION FOR A SEARCH WARRANT**

I, Tyler Fink, being first duly sworn, hereby depose and state as follows:

**I. INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for the residence located at 405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005 (hereinafter the “**SUBJECT PREMISES**”).

2. Based upon the information described below, I submit that probable cause exists that violations of Title 21 U.S.C. §§ 331(a) (interstate commerce of any misbranded drug), 331(c) (delivery of a misbranded drug), 331(d) (interstate commerce of any new drug lacking FDA approval), Title 19 U.S.C. §§ 1595a(c)(1)(B) (unlawful importation), and Title 21 U.S.C. §§ 952 (importation of a controlled substance) have been committed by Khaled SALEM (“SALEM”). I further believe that evidence of these violations will be found at the **SUBJECT PREMISES**.

3. I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found in the **SUBJECT PREMISES**, more particularly described in Attachment A. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. I am a Postal Inspector with the United States Postal Inspection Service (“USPIS”). I have been employed as a full-time law enforcement officer since June 2014.

5. The USPIS is the primary investigative arm of the United States Postal Service (“USPS”) and is charged under Title 18, United States Code, 3061 with the enforcement of laws governing the use and movement of the United States Mail, including, but not limited to, the misuse and fraudulent schemes involving the mail, crimes relating to mail fraud, identity theft, and narcotics trafficking involving the U.S. Mail.

6. I am currently assigned to the USPIS Milwaukee Office, Multi-function team, as well as being placed on the High Intensity Drug Trafficking Area (“HIDTA”) Interdiction Task Force. The USPIS Milwaukee Office investigates USPS customers involving narcotics, prohibited mailings, controlled substances, prescription medications, and other matters related to the Postal Service. I have intercepted numerous parcels, which were found to contain narcotics, prescription medications, or proceeds of narcotics trafficking and other evidence of criminal activity.

7. I hold a Bachelor of Science degree in Mechanical Engineering from the University of Missouri – St. Louis. In 2014, I completed the Peace Officer Standards and Training certification at the St. Louis County and Municipal Police Academy while employed as a City of Creve Coeur Police Officer. While working as a Police Officer, I received extensive training in narcotics investigations. In 2017, I graduated from the United States Postal Inspection Service (“USPIS”) Basic Inspector Training program. I received advanced training by the USPIS in the investigation of controlled substances or proceeds/payments being transported through the United States.

8. I have participated in numerous complex narcotics investigations which involved violations of state and federal controlled substances laws including Title 21, United States Code, Sections 841(a)(1) and 846 (possession with intent to distribute a controlled substance and conspiracy to possess with intent to distribute a controlled substance), and other related offenses. I have had both formal training and have participated in numerous complex drug-trafficking investigations, including ones using wiretaps. More specifically, my training and experience includes the following:

- a. I have used informants to investigate drug trafficking. Through informant interviews, and extensive debriefings of individuals involved in drug trafficking, I have learned about the manner in which individuals and

organizations distribute controlled substances in Wisconsin and throughout the United States;

- b. I have also relied upon informants to obtain controlled substances from dealers, and have made undercover purchases of controlled substances;
- c. I have participated in several search warrants where controlled substances, drug paraphernalia, and drug trafficking records were seized;
- d. I am familiar with the appearance and street names of various drugs, including marijuana, heroin, cocaine, cocaine base (unless otherwise noted, all references to crack cocaine in this affidavit is cocaine base in the form of crack cocaine), ecstasy, and methamphetamine. I am familiar with the methods used by drug dealers to package and prepare controlled substances for sale. I know the street values of different quantities of the various controlled substances;
- e. I am familiar with the language utilized over the telephone to discuss drug trafficking, and know that the language is often limited, guarded, and coded;
- f. I know that drug traffickers often use electronic equipment and wireless and land line telephones to conduct drug trafficking operations;
- g. I know that drug traffickers commonly have in their possession, and at their residences and other storage locations where they exercise dominion and control, firearms, ammunition, and records or receipts pertaining to such;
- h. I know that drug traffickers often use drug proceeds to purchase assets such as vehicles, property, and jewelry. I also know that drug traffickers often use nominees to purchase and/or title these assets in order to avoid scrutiny from law enforcement officials;
- i. I know large-scale drug traffickers often purchase and/or title their assets in fictitious names, aliases, or the names of relatives, associates, or business entities to avoid detection of these assets by government agencies. I know that even though these assets are in names other than the drug traffickers, the drug traffickers actually own and continue to use these assets and exercise dominion and control over them;
- j. I know large-scale drug traffickers maintain on-hand large amounts of U.S. currency to maintain and finance their ongoing drug business;
- k. I know it is common for drug traffickers to maintain books, records, receipts, notes, ledgers, airline tickets, and receipts relating to the purchase of financial instruments, and/or the transfer of funds and other papers relating to the transportation, ordering, sale, and distribution of controlled

substances. I also know that the aforementioned books, records, receipts, notes, ledgers, etc. are maintained where the traffickers have ready access to them;

- l. I know it is common for large-scale drug traffickers to secrete contraband, proceeds of drug sales, and records of drug transactions in secure locations within their residences, their businesses, storage facilities, and/or other locations over which they maintain dominion and control, for ready access and to conceal these items from law enforcement authorities or rival drug traffickers. These secure locations include, but are not limited to safes, briefcases, purses, locked filing cabinets, and hidden storage areas in natural voids of a residence;
- m. I know it is common for persons involved in large-scale drug trafficking to maintain evidence pertaining to their obtaining, secreting, transferring, concealing, and/or expenditure of drug proceeds, such as currency, financial instruments, precious metals and gemstones, jewelry, books, records of real estate transactions, bank statements and records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, safe deposit box keys, and money wrappers. These items are maintained by the traffickers within residences (including attached and unattached garages), businesses, or other locations over which they maintain dominion and control;
- n. I know large-scale drug traffickers often use electronic equipment such as telephones (land-lines and cell phones), computers, telex machines, facsimile machines, currency counting machines, and telephone answering machines to generate, transfer, count, record and/or store the information described in the items above, as well as conduct drug trafficking activities;
- o. I know when drug traffickers amass large proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits through money laundering activities. To accomplish these goals, drug traffickers utilize the following methods, including, but not limited to: domestic and international banks and their attendant services, securities brokers, professionals such as attorneys and accountants, casinos, real estate, shell corporations and business fronts, and otherwise legitimate businesses that generate large quantities of currency;
- p. I know drug traffickers commonly maintain addresses or telephone numbers in books or papers that reflect names, addresses, and/or telephone numbers of their associates in the trafficking organization; and
- q. I know drug traffickers take (or cause to be taken) and maintain photographs of themselves, their associates, their property, and their drugs.

9. In addition, during the course of residential searches, I and other agents have also found items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the subject premises. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

10. I have been the affiant on over 80 warrants in federal court. Based on my training, personal experience, on the job training, and working with other USPIS Postal Inspectors and HIDTA drug task force officers, I know narcotics, drugs, paraphernalia, controlled substances, prescription medications, and moneys associated with the sale of narcotics, drugs, and controlled substances are sent through the USPS system, and I am familiar with many of the methods used by individuals who attempt to use the USPS to illegally distribute controlled substances and prescription medications.

## **II. BACKGROUND: THE REGULATION OF DRUGS BY THE FDA AND RELATED CRIMINAL STATUTES**

### **A. General Definitions**

11. Under the Food, Drug, and Cosmetic Act (hereinafter FDCA), "interstate commerce" means commerce between any State or Territory and any place outside thereof, and commerce within the District of Columbia or within any other Territory not organized with a legislative body. 21 U.S.C. § 321(b).

12. Under the FDCA, "label" means a display of written, printed, or graphic matter upon the immediate container of any article. 21 U.S.C. § 321(k). The term "labeling" is defined as all labels and other printed or graphic matter upon any article or any of its containers or wrappers or accompanying such article. 21 U.S.C. § 321(m).

## **B. The Definition of “Drug” in the FDCA**

13. Under the FDCA, "drugs" are defined as, among other things: (a) articles intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man or other animals; (b) articles (other than food) intended to affect the structure or any function of the body of man or other animals; and (c) articles intended for use as a component of any articles specified in (a) or (b) above. 21 U.S.C. § 321(g) (1)(b)-(d).

14. A product's intended use is not determined by the intrinsic properties of the product, but by the seller's objective intent in promoting, distributing, and selling the product. *See United States v. An Article . . . "Sudden Change"*, 409 F.2d 734, 739 (2d Cir. 1969); *see also* 21 C.F.R. § 201.128. The objective intent is determined, *inter alia*, by such persons' expressions, labeling claims, advertising matter, or oral or written statements by such persons or their representatives. *See Hanson v. United States*, 417 F. Supp. 30, 35 (D. Minn. 1976), *aff'd*, 540 F.2d 947 (8th Cir. 1976); *see also United States v. Storage Spaces Designated Nos. "8"1 and "49"*, 777 F.2d 1363, 1366 (9th Cir. 1985) ("intent may be derived or inferred from labeling, promotional material, advertising, or any other relevant source."). Indeed, even water can be a drug if it is claimed to have curative properties. *See United States v. 353 Cases . . . Mountain Valley Mineral Water*, 247 F.2d 473 (8th Cir. 1957).

15. A “new drug” is any drug which is not generally recognized, among experts qualified by scientific training and experience to evaluate the safety and effectiveness of drugs, as safe and effective for use under the conditions prescribed, recommended, or suggested in the labeling thereof. 21 U.S.C. § 321(p)(1). In order to be lawfully marketed, sold or dispensed in the U.S., a new drug must be the subject of a New Drug Application ("NDA") approved by the FDA. 21 U.S.C. § 355.

16. A “prescription drug” under the FDCA is a drug that: (i) because of its toxicity and other potential for harmful effects, or the method of its use, or the collateral measures necessary to its use, was not safe for use except under the supervision of a practitioner licensed by law to administer such drug; or (ii) was limited by an application approved by FDA, to use under the professional supervision of a practitioner licensed by law to administer the drugs. 21 U.S.C. § 353(b)(1).

**C. “Misbranded Drugs” under the FDCA**

17. Dispensing a prescription drug without a valid prescription by a licensed practitioner is deemed by statute to be an act with causes the drug to be misbranded while held for sale. 21 U.S.C. § 353(b).

18. A drug is also misbranded if (a) its labeling is false or misleading in any particular, 21 U.S.C. § 352(a) or (b) its labeling does not bear adequate directions for use, 21 U.S.C. § 352(f)(11).

19. "Adequate directions for use" means directions under which a layman can use a drug safely and for the purposes for which it was intended without a doctor's supervision. 21 C.F.R. § 201.5. Directions under which a *layperson* can use a drug safely cannot be written for a prescription drug because such drugs can, by definition, only be used safely at the direction, and under the supervision, of a licensed practitioner. Approved prescription drugs dispensed pursuant to a valid prescription are exempt from having adequate directions for use by a layperson. But prescription drugs that are unapproved new drugs or dispensed without a valid prescription are necessarily misbranded for lacking adequate directions for use.



#### **D. The Criminal Penalties of the FDCA**

20. The FDCA contains several criminal provisions. Relevant here are the provisions of 21 U.S.C. § 331. Section 331(a) makes it a crime to introduce or deliver for introduction into interstate commerce any misbranded drug. Section 331(c) makes it a crime to receive in interstate commerce any misbranded drug, or to deliver or proffer the delivery for pay or otherwise any misbranded drug. Section 331(d) makes it a crime to introduce or deliver for introduction into interstate commerce any unapproved new drug. These crimes are strict-liability misdemeanors under 21 U.S.C. § 333(a)(1). *See United States v. Park*, 421 U.S. 658 (1975). But they are felonies if they are committed with an “intent to defraud or mislead” either consumers or government regulators. 21 U.S.C. § 333(a)(2).

#### **E. Other Crimes Associated with the Distribution of Drugs**

21. Other statutes aside from the FDCA criminalize behavior associated with the distribution of drugs. The mail and wire fraud statutes, for example, punish schemes to defraud or the use of false and fraudulent representations, pretenses and promises to obtain things of value executed, respectively, through the mail or interstate wires. And the Controlled Substances Act imposes criminal penalties on individuals who distribute controlled substances when not specifically authorized to do so.

### **III. SUMMARY OF PROBABLE CAUSE TO BELIEVE KHALED SALEM IS COMMITTING THE SUBJECT OFFENSES**

#### **A. First USPS Shipment Seizure**

22. The USPIS is currently investigating the shipment of misbranded prescription medication (“Subject Offense”) through the U.S. Mail.

23. On March 15, 2023, I was conducting a routine parcel screening at the Elm Grove Post Office, located at 13425 Watertown Plank Road, Elm Grove, Wisconsin 53122, when U.S.

Postal Service (“USPS”) Priority Mail parcel 9405511206223883865000 (“Subject Parcel 1”) was found to be suspicious. Subject Parcel 1 was approximately a 11.25” x 8.75” x 6” USPS parcel weighing approximately 1 lbs. 5 oz. The shipping label for Subject Parcel 1 indicated it was from “Eve Lloyd, 1801 W Oklahoma Ave, 2, Milwaukee WI 53215”. Subject Parcel 1 bore a typewritten label addressed to “Ryan Roberson, 513 US HWY 60 E, #121, Republic MO 65738”. Subject Parcel 1 was postmarked on March 15, 2023, in Elm Grove, Wisconsin 53122 at approximately 8:53 AM. The postage paid was \$12.46

24. The USPS business records indicated Subject Parcel 1 had its postage paid for using cryptocurrency through Stamps.com.

25. Based on my training and experience, a sender paying for postage with cryptocurrency may indicate the sender does not want to be associated with the parcel. Additionally, drug-traffickers will routinely mail more than one parcel containing narcotics in an effort to avoid detection.

26. Based on my training and experience, I know that individuals involved in the trafficking of illicit drugs often take advantage of the anonymity of enhanced cryptocurrency and third-party postage services such as Stamps.com.

27. Based on my training and experience, I know that drug traffickers often use enhanced cryptocurrency, such as Bitcoin, to protect their identities. Bitcoin is a decentralized digital currency without a central bank or single administrator. Payments are sent from user-to-user on the peer-to-peer bitcoin network without the need for intermediaries. Drug traffickers often use third-party postage services, such as Stamps.com, to add additional layers of anonymity to their transactions. These services allow their customers to purchase postage using cryptocurrency.

28. Based on my training and experience, multiple drug parcels mailed at the same time, likely from the same mailer, may display many of the same parcel characteristics: including weight, postage, parcel dimensions, shipping labels, and origin/destination areas.

29. While conducting the routine parcel screening at the Elm Grove Post Office and determining Subject Parcel 1 to be suspicious, I located an additional five parcels with similar characteristics as Subject Parcel 1. The additional five parcels were all paid for in cryptocurrency through Stamps.com, had the same sender's name and address as the Subject Parcel 1, and the USPS Clerk stated they were all dropped off at the same time by the same male subject who was later identified as Khaled SALEM ("SALEM").

30. On March 16, 2023, I applied for and received a federal search warrant for Subject Parcel 1. The search warrant was issued by United States Magistrate Judge Stephen Dries in the Eastern District of Wisconsin.

31. Upon executing the search warrant on Subject Parcel 1 on March 16, 2023, case agents discovered it was found to contain 20 dosage units of Human Chorionic Gonadotrophin ("HCG") injectables. Each dosage unit was pre-packaged in what appears to be its original manufactured packaging and included a vial of suspected HCG powder and a vial of a liquid labeled Sodium Chloride injection. The package indicated the HCG was manufactured in India and should not be sold "without the prescription of a Registered Medical Practitioner". The HCG was identified by its physical characteristics and packaging. The total gross weight of the suspected HCG with its packaging was approximately 387 grams.

32. On March 17, 2023, I traveled to Fazio's Chocolate, located at 13425 Watertown Plank Road, Elm Grove, Wisconsin 53122, to review surveillance video. This business is attached to the same building as the Elm Grove Post Office. The Fazio's Chocolate surveillance video for

March 15, 2023 showed SALEM entering the Elm Grove Post Office, at the same approximate postmark time for Subject Parcel 1, with several parcels and leaving several minutes later without them. SALEM was driving a dark colored Tesla sedan.

#### **B. Second USPS Shipment Seizure**

33. On March 21, 2023, I was conducting routine parcel screening at the Elm Grove Post Office, when USPS Priority Mail parcel 9405511206223852348336 (“Subject Parcel 2”) was found to be suspicious. Subject Parcel 2 was approximately an 8.5” x 5.5” x 1.75” USPS parcel weighing approximately 2 lbs. 0 oz. The shipping label for Subject Parcel 2 indicated it was from “Eve Lloyd, 1801 W Oklahoma Ave, 2, Milwaukee WI 53215”. Subject Parcel 2 bore a typewritten label addressed to “Sam Skipworth, 3948 Eagle Nest Lake Lane, Magnolia TX 77354”. Subject Parcel 2 was postmarked on March 21, 2023, at Elm Grove, Wisconsin 53122 at approximately 9:41 AM. The postage paid was \$7.21

34. The USPS business records indicated Subject Parcel 2 had its postage paid for using cryptocurrency through Stamps.com.

35. On March 21, 2023, I applied for and received a federal search warrant for Subject Parcel 2. The search warrant was issued by United States Magistrate Judge Stephen Dries in the Eastern District of Wisconsin.

36. Upon executing the search warrant on Subject Parcel 2, on March 22, 2023, case agents discovered Subject Parcel 2 was found to contain 50 vials, or dosage units, of an off-white powdery substance with no labeling on the vials. The unknown powder was field tested and indicated positive for hydroxyzine pamoate. Hydroxyzine pamoate is a prescription medication. The total gross weight of the powder with its packaging was approximately 346 grams.

37. On March 21, 2023, I traveled to Fazio’s Chocolate to review surveillance video. The Fazio’s Chocolate surveillance video for March 21, 2023 showed SALEM taking multiple

parcels out of his Tesla and walk towards the blue collection boxes outside of the Elm Grove Post Office at the same approximate postmark time for Subject Parcel 2. A short time later the surveillance video showed SALEM returning to his Tesla without the parcels.

### **C. USPS Regulations**

38. The USPS Publication 52 regulations provide that prescription medicines are permitted to be sent via the U.S. mail only by a drug manufacturer or their registered agents, pharmacies, medical practitioners, or other authorized dispensers as permitted. The inner packaging of the controlled substance is required to be marked to show the prescription number and the name and address of the pharmacy, practitioner, or other person dispensing the prescription and must be securely held within a plain outer wrapper or packaging.

39. Subject Parcel 1 and Subject Parcel 2, containing suspected prescription medications, did not appear to be sent by any of the authorized agents described above and did not follow the packaging requirements.

40. A search of the Wisconsin Department of Safety and Professional Services indicated SALEM is not currently a licensed doctor, pharmacist, or physician who would have the authority to prescribe medications.

### **D. Identification of Khaled SALEM**

41. While executing the search warrant on Subject Parcel 1, the cardboard box used to ship the contents of Subject Parcel 1 appeared to be a reused box. On one corner of the box was a USPS postage label that appeared to be partially ripped off, but it still showed a postage paid of \$17.10 at the Las Vegas, Nevada 89103 Post Office. Additionally, it indicated a destination zip code of Brookfield, Wisconsin 53005. The shipping label for Subject Parcel 1 was taped over the original shipping label placed on the box prior to this shipment. The original shipping label

indicated it was from “revive, 150 hoover ave, las vegas, NV 89101” and the destination name and address was partially removed and blacked out with a marker.

42. I interviewed the Elm Grove Post Office Supervisor who stated Subject Parcel 1 was dropped off by what appeared to be a Middle Eastern male with a muscular build, dark hair, and “olive” skin complexion. The Supervisor said the male subject was driving a dark colored Tesla sedan with a possible license plate of “ABD9023”, but he stated the “B” was hard to read and could have been a different letter.

43. A review of the Wisconsin Department of Transportation database indicated a 2018 Tesla Model S bearing ARD9023 was registered to a Khaled Shawkat SALEM at 405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005 (i.e., the **SUBJECT PREMISES**).

44. I reviewed the USPS business records for SALEM’s listed residence, 405 Bishops Way Apartment 223, which showed USPS Priority Mail parcel 9505510048983066836752 was shipped from Las Vegas, Nevada 89103 on March 7, 2023, and was delivered on March 9, 2023. A review of the shipping label indicated it was from “revive, 150 hoover ave, las vegas, NV 89101”. This information matches what is shown on the original shipping label placed on the cardboard box of Subject Parcel 1. An image of the shipping label for parcel 9505510048983066836752 showed it was addressed to “Khaled Salem, 405 Bishops Way apt 223 Brookfield Wi 53005”.

45. On March 17, 2023, I showed the Elm Grove Postal Supervisor the Wisconsin driver’s license photo of SALEM. The Supervisor confirmed SALEM was the person who shipped Subject Parcel 1 and Subject Parcel 2.

#### **E. Subpoena Return on SUBJECT PREMISES**

46. On March 17, 2021, case agents served a subpoena on Brookfield Reserve, 405 Bishops Way, Brookfield, Wisconsin, requesting a current customer list. The subpoena return

showed SALEM is the current renter of Apartment 223 (i.e., the **SUBJECT PREMISES**). Additionally, the records showed SALEM's vehicle information as a gray 2018 Tesla Model S with a license plate of ARD9023.

#### **F. Surveillance at the SUBJECT PREMISES**

47. I have conducted surveillance in the early morning hours at 405 Bishops Way on multiple occasions. SALEM's Tesla has consistently been observed parked on the second floor of the apartment complex's parking garage.

48. On April 3, 2023, at approximately 8:30 AM, I was conducting surveillance at 405 Bishops Way when I observed SALEM exit his Tesla and use what appeared to be a key fob to open the door to leave the parking garage and enter the residential area of the apartment complex. The Property Manager for the apartment complex advised all of their residents were provided key fobs to access the building from the parking garage.

#### **G. Historical USPS Records**

49. The USPS records have indicated that between the dates of January 16, 2023 through March 29, 2023, there have been 89 parcels shipped from multiple Post Offices in the same vicinity as the **SUBJECT PREMISES** with similar characteristics as Subject Parcel 1 and Subject Parcel 2.

50. All of these parcels had their postage paid for in cryptocurrency through Stamps.com and they had a sender's address of 1801 W. Oklahoma Ave, Milwaukee, Wisconsin from either apartment 1 or 2. The majority of these parcels' labels showed the sender's name as "Eve Lloyd". Some of the parcels did not list a sender's name.

51. The Consolidated Lead Evaluation and Reporting ("CLEAR") database is a public records product which is designed for law enforcement officers in locating subjects and witnesses, verifying identities of individuals, and gathering background information for use in investigations.

A search of the CLEAR database revealed no person by the name of Eve Lloyd currently lives, or has lived, at 1801 W. Oklahoma Avenue Apartment 2, Milwaukee Wisconsin 53215. This same database revealed no person named Eve Lloyd has lived at 1801 W. Oklahoma Avenue or any apartment number within the apartment building.

52. This same database indicated SALEM once utilized 1801 W. Oklahoma Avenue, Apartment 2, Milwaukee, Wisconsin as his address.

53. On March 23, 2023, I was reviewing historical USPS records for the **SUBJECT PREMISES** when Subject Parcel 3 and Subject Parcel 4 (as described below) were found to be suspicious.

54. The first suspicious historical parcel delivered to the **SUBJECT PREMISES** was USPS Priority Mail parcel 9405511206223885970979 ("Subject Parcel 3"). Subject Parcel 3 was approximately a 12" x 9" x 1" USPS parcel weighing approximately 4 lbs. 0 oz. The shipping label for Subject Parcel 3 indicated it was from "Ronald Hydrafist, 4940 Tanners Spring Dr, Alpharetta GA 30022". Subject Parcel 3 bore a typewritten shipping label addressed to "Khaled Salem, 405 Bishops Way, 223, Brookfield WI 53005". Subject Parcel 3 was postmarked on February 22, 2023, in Alpharetta, Georgia 30320. Subject Parcel 3 was delivered on February 28, 2023, at approximately 11:19 AM.

55. A search of the CLEAR database revealed no person by the name of Ronald Hydrafist currently lives, or has lived, at 4940 Tanners Spring Dr, Alpharetta GA 30022.

56. The second suspicious historical parcel delivered to the **SUBJECT PREMISES** was USPS Priority Mail parcel 9405511206223883787104 ("Subject Parcel 4"). Subject Parcel 4 was approximately an 8.69" x 5.44" x 1.75" USPS parcel weighing approximately 0 lbs. 10 oz. The shipping label for Subject Parcel 4 indicated it was from "Brian Wood, 82863 Western Way



Cir, Jacksonville FL 32256-0369". Subject Parcel 4 bore a typewritten label addressed to "Bryce Kappes, 405 Bishops Way, Apt 223, Brookfield WI 53005". Subject Parcel 4 was postmarked on March 16, 2023, in Jacksonville, Florida 32099. The postage paid was \$7.21. Subject Parcel 4 was delivered on March 20, 2023, at approximately 11:28 AM.

57. A review of USPS records indicated the sender's address shown on the shipping label of Subject Parcel 4 was a fictitious address.

58. The USPS business records indicated Subject Parcel 3 and Subject Parcel 4 had their postage paid for with cryptocurrency through Stamps.com.

#### **H. Historical U.S. Customs and Border Protection Seizures**

59. A review of seizures made by Customs and Border Protection ("CBP") showed multiple parcels intended for the **SUBJECT PREMISES** addressed to SALEM were seized by CBP.

60. On April 13, 2022, the Chicago, Illinois CBP office seized USPS parcel LA243742955EE ("Subject Parcel 5"). Subject Parcel 5 was mailed from Estonia and was being shipped to Khaled Salem, 405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005 (i.e., the **SUBJECT PREMISES**). The CBP record shows Subject Parcel 5 contained approximately 100.9 grams of Testosterone Cypionate ampoules (250mg/ml) 10 ml. Testosterone Cypionate is an anabolic steroid medication and is a Schedule III controlled substance per the Controlled Substance Act.

61. The same CBP seizure indicated Subject Parcel 5 also contained approximately 400 Oxandrolone 10mg tablets with an approximate weight of 110.7 grams. Oxandrolone is an anabolic steroid medication and is a Schedule III controlled substance per the Controlled Substance Act.

62. The importation of the controlled substances found in Subject Parcel 5 violates Title 19 U.S.C. §§ 1595a(c)(1)(B) (unlawful importation) and 21 U.S.C. §§ 952 (importation of a controlled substance).

63. On December 13, 2022, the Memphis, Tennessee CBP office seized FedEx parcel 590185958791 (“Subject Parcel 6”). Subject Parcel 6 was mailed from Turkey and was being shipped to Khaled Salem, 405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005 (i.e., the **SUBJECT PREMISES**). The CBP record shows Subject Parcel 6 contained approximately 53.7 grams of Koriogonadotropin 0.5 ml injectables. An open-source database check indicated Koriogonadotropin is another form of HCG which is the same prescription drug seized from Subject Parcel 1 shipped by SALEM.

64. The same CBP seizure indicated Subject Parcel 6 also contained approximately 304.7 grams of Metformin 1000mg tablets. Metformin is a prescription medication used to treat high blood sugar levels that can cause diabetes. An open-source database check indicated it is also used by bodybuilders while attempting to lose weight.

65. The unauthorized importation of the prescription medication found in Subject Parcel 6 violates Title 19 U.S.C. §§ 1595a(c)(2)(A) (unlawful importation) and Title 42 U.S.C. §§ 262 (regulation of biological products).

#### **IV. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

66. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

67. *Probable cause.* I submit that if a computer or storage medium is found on the **SUBJECT PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

68. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe

that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data

typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to operate a website that is used for illegal conduct, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal

conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

69. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a property for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the **SUBJECT PREMISES**, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the **SUBJECT PREMISES** could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the **SUBJECT PREMISES**. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

70. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

71. Because multiple people may share the **SUBJECT PREMISES** as a residence, it is possible that the **SUBJECT PREMISES** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

#### **IV. BIOMETRIC ACCESS TO DEVICES**

72. This warrant permits law enforcement to compel residents of the **SUBJECT PREMISES** to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five



fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

- c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.
- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.
- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Affidavit, I believe one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some



circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Khaled SALEM or other residents of the **SUBJECT PREMISES** to the fingerprint scanner of the devices; (2) hold the devices found in front of the face of Khaled SALEM or other residents of the **SUBJECT PREMISES** and activate the facial recognition feature; and/or (3) hold the devices found in front of the face of Khaled SALEM or other residents of the **SUBJECT PREMISES** and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Khaled SALEM or other residents of the **SUBJECT PREMISES** state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to compel Khaled SALEM or other residents of the **SUBJECT PREMISES** to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

### **CONCLUSION**

73. Based on the foregoing, I respectfully request that this Court issue a search warrant for the location described in Attachment A authorizing the seizure and search of the items described in Attachment B.

## ATTACHMENT A

### **405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005**

405 Bishops Way, Apartment 223, Brookfield, Wisconsin 53005 is a residential unit in an apartment complex having a multi-colored stone structure, off-white colored trim, and a black and white roof. The numbers “405” are affixed to the apartment complex sign on the east side of the building. Apartment 223 is located on the second floor inside the apartment complex. The number “223” is displayed in black lettering next to the interior entrance door to the residential unit. Images of the exterior of the apartment complex and the entrance to Apartment 223 are below:



## **ATTACHMENT B**

### **Particular Things to be Seized**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, or property designed or intended for use or which is or has been used to assist in obtaining the means of committing criminal offenses, namely violations of Title 21 U.S.C. §§ 331(a) (interstate commerce of any misbranded drug), 331(c) (deliver of a misbranded drug), 331(d) (interstate commerce any unapproved new drug lacking FDA approval), Title 19 U.S.C. §§ 1595a(c)(1)(B) (unlawful importation), and Title 21 U.S.C. §§ 952 (importation of a controlled substance), hereinafter identified as the SUBJECT OFFENSES.

- a. Records and information relating to the purchase, sale, shipment, handling, importation, or distribution of Human Chorionic Gonadotrophin (“HCG”), and any other controlled substance, unapproved new drug products, misbranded drug products, and drug products unlawfully imported into the United States, including but not limited to prescriptions, bills, invoices, bills of lading, shipping documents, purchase orders, letters, notes, and order forms;
- b. Records and information, including literature, advertising, and labeling, related to the administration of HCG, any other controlled substance, unapproved new drug products, misbranded drug products, or drug products unlawfully imported into the United States, including related correspondence and communications;
- c. Records and information concerning the acquisition, retention, or distribution of HCG, any other controlled substance, unapproved new drug products, misbranded drug products, or drug products unlawfully imported into the United States, including related correspondence and communications;
- d. Records and information reflecting payment, receiving payment, or other transfer of funds in connection with the SUBJECT OFFENSES, including the acquisition, purchase, procurement, disbursement, or distribution of HCG, any other controlled substance, unapproved new drug products, misbranded drug products, or drug products unlawfully imported into the United States, such as checks, money orders, financial records, bank statements, currency, or other financial documents;

- e. Firearms, ammunition, cases, or firearm accessories and documents showing firearm possession or ownership, to include but not limited to CCW permit and firearm purchase/acquisition documents;
- f. Indicia of unlawful possession, use, or distribution of controlled substances and prescription medication, including but not limited to paraphernalia and evidence known to be associated with drug trafficking and/or drug possession;
- g. USPS packages or boxes;
- h. Evidence of recent cash expenditures;
- i. Information regarding identification and location of assets obtained with drug proceeds;
- j. Documents or other items pertaining to the controlled substance and prescription medication customers;
- k. All records, items, and documents reflecting travel for the purpose of participating in the aforementioned criminal offense, including but not limited to gas station receipts, store receipts, credit card receipts, restaurant receipts, maps, and records of long distance calls reflecting travel;
- l. All computers, tablets, and cellular telephones which may have been used by Kahled SALEM which may contain travel records, contacts with other individuals, email or social media contacts, or other records or communications related to the SUBJECT OFFENSES;
- m. Accounting records, specifically financial statements, bank records, ledgers, journals, check registers, and other books and records used to maintain a record of income and expenses;
- n. Checking, savings, and investment account records, including signature cards, account statements, deposit receipts, withdrawal receipts, cancelled checks, money orders, cashier's checks, records of incoming and outgoing wire transfers, electronic funds transfer records, checkbooks, credit card records and receipts, including supporting documentation and schedules, and any other records of documents pertaining to the receipt, expenditure, or concealment of money;
- o. Any and all of the above listed evidence stored in the form of magnetic or electronic coding on computer media or media capable of being read by a computer or with the aid of computer-related equipment, including but not limited to floppy disks, fixed hard

- disks, removable hard disks, tapes, laser disks, videocassettes, CD-ROM's, DVD disks, Zip disks, smart cards, memory sticks, memory calculators, personal digital assistants (PDS's), cell phones, and/or other media capable of storing magnetic coding, the software to operate them and related instruction manuals;
- p. All electronic devices which are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer impulses or data. These devices include computers, computer components, computer peripherals, word processing equipment, modems, monitors, printers, plotters, encryption circuit boards, optical scanners, external hard drives, and other computer related electronic devices;
  - q. All indicia of occupancy, residency or ownership of the premises and things described in the warrant, including identification documents, utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents, and keys.
  - r. Paraphernalia associated with the manufacture and distribution of controlled substances and prescription medications including but not limited to materials and items used for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, and heat-sealing devices;
  - s. Proceeds of drug trafficking activities, such as United States currency, precious metals, financial instruments, and jewelry, and documents and deeds reflecting the purchase or lease of real estate, vehicles, precious metals, jewelry or other items obtained with the proceeds from drug trafficking activities;
  - t. Drug or money ledgers, drug distribution or customer lists, drug supplier lists, correspondence, notations, logs, receipts, journals, books, records, and other documents noting the price, quantity, and/or times when controlled substances were obtained, transferred, sold, distributed, and/or concealed;
  - u. Records of off-site storage locations, including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;
  - v. Indicia of occupancy, residency or ownership of the premises and things described in the warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents and keys;

For any computer, cell phone, tablet, or storage medium (hereinafter, for purposes of this Attachment B, collectively referred to as a “COMPUTER”) whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the COMPUTER was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the COMPUTER user’s state of mind as it relates to the SUBJECT OFFENSES;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;

- l. records of or information about the COMPUTER's internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment; and
- n. Routers, modems, and network equipment used to connect a COMPUTER to the internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "COMPUTER" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, flash memory, CD-ROMs, and other magnetic or optical media.